

# FIREWALL UND KOMMUNIKATIONSMATRIX E-CONNECT

Version: 1.4



# Inhaltsverzeichnis

<b>1.</b>	<b>Einleitung</b>	<b>1</b>
<b>2.</b>	<b>Firewall und Kommunikationsmatrix e-connect</b>	<b>2</b>
2.1.	Tabellarische Übersicht Firewall und Kommunikationsmatrix	2
2.2.	Allgemeine Protokolle und Ports	5

Sehr geehrte Nutzer,

die folgende Tabelle zeigt Vorgaben, welche in der Firewall und Antivirensoftware berücksichtigt werden müssen, damit eine reibungslose Kommunikation zwischen den einzelnen e-connect-Softwarekomponenten möglich ist.

Bitte beachten Sie, dass e-connect für Microsoft Windows 10 (64Bit) getestet und freigegeben wurde. Für die Installation der Software werden erhöhte Benutzerrechte (Administrator) benötigt. Die Software selbst kann im Benutzerkontext genutzt werden.

Bei Fragen oder Anregungen wenden Sie oder Ihr Systembetreuer sich an [ti-technik@dampsoft.de](mailto:ti-technik@dampsoft.de).

Vielen Dank

Ihr e-connect-Team

---

## **Hinweis!**

**Bitte nehmen Sie die Einstellungen der Firewall und Antivirensoftware am Tag der Installation von e-connect vor dem Installationstermin vor, um eventuelle Ausfallzeiten zu minimieren und eine reibungslose Installation zu ermöglichen. Ziehen Sie dazu Ihren Systembetreuer hinzu.**

---

### 2.1. Tabellarische Übersicht Firewall und Kommunikationsmatrix

#### Hinweis!

Das Kartenterminal in Ihrem Netzwerk muss mit dem Rechner, auf dem der TIC installiert ist, einwandfrei kommunizieren können. In den Einstellungen der lokalen Firewall auf diesem Rechner müssen die im TIC unter „PROXY-PORT“ angezeigten Ports freigeschaltet werden. In der Regel sind dies UDP/TCP-Ports zwischen 9000 und 9020.

Komponente	Sichtweise	Service	Port	Protokoll	Kommentar	eingehend	ausgehend	Quelle	Ziel
TIC	Richtung Internet	VPN-Verbindung Konnektor	60000 bis 60100	TCP/UDP	Verbindung zum VPN-Endpunkt für Verbindung zum Konnektor	Ja	Ja	Lokaler Client	vpn.pu.tiaas.rise-ti.de
TIC	LAN	Kommunikation mit Kartenleser	Kartenleser 4742	TCP/UDP	Kommunikation zwischen TIC auf installierten PC-System zum Kartenleser	Ja	Ja	Lokaler Client	Kartenleser
TIC	Richtung Internet	TIC-Self-Update-Server	443	TCP	Kommunikation zum Update-Server der TIC-Installation	Ja	Ja	Lokaler Client	<a href="https://client.rise-tiaas.de">https://client.rise-tiaas.de</a>
TIC	LAN	Verzeichnisdienst	636	TCP	LDAP-Proxy des V-Konnektors zum TI-Verzeichnisdienst	Nein	Ja	Lokaler Client	konnektor.pu.tiaas.rise-ti.de (10.156.120.103)
KIMaaS	LAN	SMTPPort	1500	TCP	SMTP-Port über den die Clients auf den SMTP-Proxy des KIMaaS zugreifen	Ja	Ja	Lokaler Client	kim.pu.tiaas.rise-ti.de (10.156.120.103)

Komponente	Sichtweise	Service	Port	Protokoll	Kommentar	eingehend	ausgehend	Quelle	Ziel
KIMaaS	LAN	POP3-Port	1600	TCP	POP3-Port über den die Clients auf den SMTP-Proxy des KIMaaS zugreifen	Ja	Ja	Lokaler Client	kim.pu.tiaas.risetti.de (10.156.120.103)
KIMaaS	LAN	Verzeichnisdienst	636	TCP	SMTP-Port über den die Clients auf den SMTP-Proxy des KIMaaS zugreifen	Nein	Ja	Lokaler Client	V-Konnektor via TlaaS VPN
KIM via KCM	LAN	SMTPPort	465	TCP	SMTP-Port über den die Clients auf den SMTP-Proxy des KIMaaS zugreifen	Ja	Nein	Lokaler Client	Lokaler KCM-Client
KIM via KCM	LAN	POP3-Port	995	TCP	POP3-Port über den die Clients auf den SMTP-Proxy des KIMaaS zugreifen	Ja	Nein	Lokaler Client	Lokaler KCM-Client
KIM via KCM	Richtung Internet	Arvato Account-Manager	443	TCP	Account-Manager, welcher für die Registrierung/Verwaltung von KIM-Postfächern verwendet wird	Nein	Ja	Lokaler Client	<a href="https://am.kimp-lus.de">https://am.kimp-lus.de</a>

Komponente	Sichtweise	Service	Port	Protokoll	Kommentar	eingehend	ausgehend	Quelle	Ziel
KIM	Richtung Internet	RISE-Onboarding-Service	443	TCP	Wird für die Registrierung von KIM-Postfächern verwendet.	Nein	Ja	Lokaler Client	<a href="https://ops.rise-kim.de">https://ops.rise-kim.de</a>
KIM	Richtung Internet	OCSP Responder	80	TCP	OCSP Responder der für die Prüfung des Zertifikates von <a href="https://am.kimplus.de">https://am.kimplus.de</a> erreichbar sein muss	Nein	Ja	Lokaler Client	<a href="http://status.geotrust.com">http://status.geotrust.com</a>
OS	LAN	KT-Proxy Port	ab Port 9000	TCP/UDP	Für die Kommunikation zwischen Kartenleser und lokalem Client	Ja	Ja	Lokaler Client	Kartenleser
DS-Win	LAN	automatisches Kartenlesen	im DS-Win konfigurierbar (1313)	TCP	für das automatische Kartenlesen im DS-Win	Ja	Nein	Lokaler Client	Lokaler Client

### 2.2. Allgemeine Protokolle und Ports

Komponente	Sichtweise	Service	Port	Protokoll	Kommentar	eingehend	Ausgehend	Quelle	Ziel
DNSSec			53	TCP/UDP		Nein	Ja		
HTTP			80	TCP		Nein	Ja		
HTTPS			443	TCP		Nein	Ja		
IKE			500	UDP		Nein	Ja		
NAT-Traversal			4500	UDP		Nein	Ja		
HTTPS			8443	TCP		Nein	Ja		

